

## Foundations of Cryptography

Cryptography is an art become science discipline that pervades the contemporary communication information infrastructure. It has a rich history within many forms but it is only relatively recently that it has moved into a science as the need for standards has arisen.

The talk will cover what the speaker believes are the basic tenets of cryptography. These tenets will be interwoven with the basic genres of cryptography. It is the speaker's belief that there are only a few basic such tenets and it is his goal to present them in a form and context that can be easily grasped.

Some related areas will also be touched upon. These include steganography, the hiding of messages within larger, overtly innocent texts, and the concept of the subliminal channel. The former topic is gathering much attention as the field of digital rights management continues to expand at a frenetic pace. The subject is also of interest to those concerned with national security measures.

The speaker will not assume that the audience is proficient in probability theory although an appreciation of elementary probability should enable the audience to better contextualize the concepts and results.

## IEEE Online Communities

When IEEE was founded, its members could easily get together for face-to-face, real time communication due to their location. But, as the membership of the Institute grew, efforts had to be made to increase the participation of those living in other parts of the country. Additionally, as the scope of electrical engineering expanded, engineers became more specialized and sought to exchange information with others in the same specialties. It was this need to interact that led to the formation of the first Technical Committee in 1903.

Through the means of new technology, we can now bridge geographical boundaries and provide additional opportunities for IEEE Members to communicate and collaborate through use of Online Communities.

An Online Community consists of a group of individuals that have a shared purpose or common interests that utilize online communication and collaboration tools to facilitate the accomplishment of their goals or to fill voids that may currently exist by relying solely on in-person or real-time interactions. Online Community Members are engaged in value-creating relationships with "anytime/anywhere" access to shared knowledge. Through the use of tools in the software platform, community members interact socially, which facilitates a sense of togetherness.

Some benefits of Online Communities are:

- Online collaboration and continued communication outside of in-person meetings and teleconferences.
- Networking opportunities
- Discussions on the latest technologies, vital issues, and IEEE activities
- Just-in time education for application on the job
- Access to technical experts and peers for advice, and problem-solving
- Peer review of work

At IEEE, the goal of online collaboration is to call forth the best that members have to offer one another and minimize all of the obstacles that we can in order for this exchange to occur.

IEEE delivers tools and methods for online collaboration so that each community can quickly focus on vital issues or projects at hand, operate in a cost-effective manner, enhance continuity of effort, clarify and gain consensus through dialog, create synergistic interdependence with other IEEE constituencies and create valuable resources.

IEEE invites you to be our Guest and come and view the Online Communities. If you like what you see and are interested in joining, you can do so for FREE!

To preview or join any of the IEEE Online Communities visit:

<https://www.ieeeonlinecommunities.org>

## Foundations of Cryptography

Featuring: Dr. John Hershey

Monday, March 8<sup>th</sup>, 6:30 pm  
Mayo Medical Sciences Building  
(321 3<sup>rd</sup> Avenue SW, Rochester)

▶ Pizza at 6:30; Meeting at 7:00 ◀

*Sponsored by  
the Southern Minnesota Section  
IEEE Joint Chapter in Communications, Signal Processing, and  
Control Systems Societies  
and  
the Southern Minnesota Section  
IEEE Computer Society Chapter*

John Hershey holds a PhD degree in electrical engineering. He is adjuncted at the Rensselaer Polytechnic Institute and at Union College. He is the author/coauthor of seven books. He and Rao Yarlagadda were the first editors-in-chief of Academic Press' journal "Digital Signal Processing" which they started in 1991. He holds 89 issued US Patents and has 39 US patent applications pending. He is an elected fellow of the IEEE "for contributions to secure communications."

## MSU IEEE Job Fair

by Andy Kim

Minnesota State University, Mankato  
Thursday, April 8, 2004  
9AM-2PM

Employers and professionals: mark your calendar now for the MSU IEEE job fair!

The job fair is intended to give employers an intimate look at the potential which has been developing within the ECET department at MSU over the last four years. It is focused exclusively on giving employers direct contact with both graduate and undergraduate students with majors in Electrical Engineering and Technology and Computer Engineering and Technology.

The job fair is an effective way to gain company recognition among future graduates even if not currently hiring.

For details, please see the brochure at:

[www.ewh.ieee.org/r4/southern\\_minnesota/](http://www.ewh.ieee.org/r4/southern_minnesota/)

## IEEE Pre-college Educator Award

Nominations are open for the IEEE Pre-college Educator Award. Colleagues of pre-college educators who have inspired in their students an appreciation and understanding of mathematics, science and technology, and engineering are encouraged to nominate that individual for the 2004 IEEE Pre-College Educator Award. Qualified candidates must be current pre-college classroom teachers. The award consists of a US\$1,000 honorarium and plaque. The deadline for nominations is 30 April. To nominate a colleague, visit [IEEE Educational Activities](http://www.ieee.org/organizations/cab/EBAwards/awardprecollege-2004.htm).

([www.ieee.org/organizations/cab/EBAwards/awardprecollege-2004.htm](http://www.ieee.org/organizations/cab/EBAwards/awardprecollege-2004.htm))

## Embedded Systems Conference

IEEE members who register by 25 March for the electronicaUSA Embedded Systems Conference (ESC) to be held 29 March - 1 April in San Francisco, receive a 25 percent discount on the registration fee. Intended for engineers and engineering managers who develop products that incorporate processor-based technology, ESC is structured as an educational forum with 132 classes on the trends, tools and methodologies of the industry. Through a media partnership with electronicaUSA, *IEEE Spectrum* and IEEE Membership will host a booth on the exhibition floor at the conference. To register for the conference, visit [ESC](http://ESC).  
([www.esconline.com/electronicaUSA/tech\\_conf/esc/](http://www.esconline.com/electronicaUSA/tech_conf/esc/))

## Exhibit on World War II Technologies

The IEEE Virtual Museum has launched an exhibit on World War II technologies. "World War II: How War Impacted Technology; How Technology Impacted War" includes a primer on the causes of the war, technologies that transformed the way war was fought, technologies that grew out of wartime urgency, and facts about the people who created the technologies. To view the new exhibit, visit the [IEEE Virtual Museum](http://IEEE Virtual Museum).  
([www.ieee.org/museum](http://www.ieee.org/museum))



**The Institute of Electrical  
and Electronics Engineers, Inc.  
Southern Minnesota Section**

**Dated Material – Please Delivery Immediately**

## IEEE Biomedical Library

Ovid Technologies and the IEEE have introduced the IEEE Biomedical Library. The collection of more than 40,000 documents from IEEE and the Institute of Electrical Engineers is available to subscribers to the Journals@Ovid database. Users may access tables of contents and bibliographic citations, link from bibliographic databases, and link between full-text articles. The IEEE Biomedical Library includes articles on analytical diagnostic techniques, bioinformatics, biomechanics, genetics, hospital engineering, medical imaging, nanobioscience, neuroengineering, prosthetics and orthotics, sensory processing, speech and biocommunications, and therapeutic surgical techniques, among others. To arrange for a free trial, contact [Ovid](http://Ovid). ([sales@ovid.com](mailto:sales@ovid.com))

## April Meeting Topic

### A new solution to Public Transportation

Presented by Dr. J. Edward Anderson, Ph.D, P.E.

**Non-Profit**  
U.S. Postage Paid  
Permit #511  
Rochester, MN

### IEEE Southern Minnesota Section Board Members

Chair	Jason Clegg	253-2369	<a href="mailto:j.clegg@ieee.org">j.clegg@ieee.org</a>
Vice Chair	Rob Harveland	253-0780	<a href="mailto:r.harveland@ieee.org">r.harveland@ieee.org</a>
Secretary	Bill Gorder	282-2029	<a href="mailto:w.gorder@ieee.org">w.gorder@ieee.org</a>
Treasurer	Steve Kerchberger	322-9202	<a href="mailto:s.kerschberger@ieee.org">s.kerschberger@ieee.org</a>
Comm/SP/CS Society	Nick Chbat	284-5118	<a href="mailto:chbat@mayo.edu">chbat@mayo.edu</a>
Comm/SP/CS Society	Scott Dahl	253-0428	<a href="mailto:ssdahl@us.ibm.com">ssdahl@us.ibm.com</a>
Computer Society	Ron Jensen	253-3887	<a href="mailto:r.jensen@ieee.org">r.jensen@ieee.org</a>
Membership	Jim Carey	253-0193	<a href="mailto:jecarey@ieee.org">jecarey@ieee.org</a>
Newsletter	Dennis Spathis	271-6894	<a href="mailto:djspathis@ieee.org">djspathis@ieee.org</a>
Educational Activities	Vince Lynch	433-0456	<a href="mailto:vmlynch@smig.net">vmlynch@smig.net</a>
Student Activities	Andy Kim	253-2409	<a href="mailto:andykim@us.ibm.com">andykim@us.ibm.com</a>
Communications	Diane Manlove	253-7613	<a href="mailto:dmanlove@ieee.org">dmanlove@ieee.org</a>

[www.ewh.ieee.org/r4/southern\\_minnesota](http://www.ewh.ieee.org/r4/southern_minnesota)

## Puzzler

How can you obtain water at 72° using only these three containers and nothing else? The 3-liter container is empty. The 5-liter container is full of 50° water and the 6-liter container is full of 90° water.

